Занятие №2
Тема: Финансовая безопасность: нет мошенникам и сомнительным схемам

Цели занятия:
- закрепить знания слушателей о финансовом мошенничестве;
- показать важность насмотренности и критического мышления при принятии финансовых решений;
- умение использовать теорию в реальной жизни, следуя советам на каждый день

Возраст участников: 18+ лет
Количество участников в группе: до 12 человек
Продолжительность занятия: 90 минут

Дидактические средства:
- презентация к занятию №2
- рабочая тетрадь
- карточки к Практикуму «Обмани меня, если сможешь» (распечатать все карточки по 1 шт)
- видео «Письмо счастья» https://www.youtube.com/watch?v=ILvYbw96-5k
- советы на каждый день
- видео в уроке:
  https://www.youtube.com/watch?v=qZAejyN9Hxo
  https://www.youtube.com/watch?v=WFMPHNHAoAQ
  https://www.youtube.com/watch?v=quJoYsaVtiY

Сценарий проведения занятия

1. Приветствие, настройка на занятие - 10 мин.

Цель: рассказать участникам о теме занятия, объяснить правила поведения, настроить на занятие

Всем добрый день! Меня зовут — *(имя ведущего)*. Это моя коллега *(имя коллеги.)* Сегодня мы будем проводить для вас занятие по финансовой грамотности. Сегодня нас … человек, и я предлагаю озвучить правила работы в группе: - Один говорит, другие слушают. - Относимся друг к другу с уважением и дружелюбно. - Глупых вопросов не бывает – самые глупые вопросы те, которых не задали. - Если что-то непонятно - переспроси!	
Тема занятия у нас животрепещущая: **финансовая безопасность.** А что такое безопасность, кто может ответить? *(ответы слушателей)*	Слайд 1 (тема)
Да, безопасность - это состояние, когда нам ничего не угрожает. А если мы говорим о финансовой безопасности - это состояние, когда нашим деньгам ничего не угрожает. Они находятся под защитой от финансовых мошенников. Правда, иногда нам приходится защищать деньги и от самих себя. Потому что большинство мошеннических схем построены так, что человек добровольно отдает деньги мошенникам. Удивлены? Давайте разбираться.	Слайд 2
Кто знает, что такое мошенничество? *Слушаем ответы.*	Слайд 3
Давайте спросим у нашего эксперта Ирины. Ирина - финансовый консультант. Она поможет нам разобраться в теме.	Слайд 4
Озвучка голоса Ирины на слайде: Финансовое мошенничество – это когда кто-то обманывает других людей, чтобы украсть их деньги. Есть разные способы такого мошенничества. Например, мошенник может втереться к вам в доверие и узнать ваши личные данные или выманить деньги другим способом. Также мошенники могут обмануть вас, предоставив ложную информацию, заставляя вас совершить какое-либо действие, которое приведёт к потере денег.	Нажмите на «плей»
Отличия от обычной кражи В отличие от обычного воровства, при финансовом мошенничестве преступники получают чужие деньги хитростью, без насилия. Жертвы сами отдают деньги мошенникам, потому что думают, что получат что-то полезное, например, дом, вещи или наследство. Но на самом деле никаких подарков нет, люди просто теряют свои деньги. Преступники с самого начала знают, что у них нет прав на эти деньги. *Тренер:*	Слайд 5 Нажмите на «плей»

Сейчас мошенники используют не только новые технологии, но и психологические приёмы, чтобы обманывать людей и забирать их деньги. Из-за своей доверчивости на уловки мошенников попадаются и молодёжь, и пожилые люди, и те, у кого нет образования, и даже учёные. Любой доверчивый человек может потерять свои деньги.
Расскажите, слышали ли вы о финансовом мошенничестве? Предлагаю обсудить ваш жизненный опыт.
Расскажу про себя. Недавно моя подруга чуть не стала жертвой мошенничества.
Ей позвонил сотрудник службы безопасности банка и огорошил заявлением о том, что с её карты прямо сейчас пытаются списать крупную сумму, и, чтобы этого не случилось, необходимо назвать номер карты, CVV-код и код из СМС.
Хорошо, что она позвонила мне посоветоваться, и нам удалось сохранить ее деньги.
Сталкивались ли вы или ваши знакомые с подобными ситуациями? Расскажите.
Тренер обращается к слушателям. Слушатели отвечают.

После обсуждения включаем слайд с Дмитрием, у которого тоже есть мнение на этот счет.
Озвучка голоса Дмитрия на слайде:
Привет, друзья! Возможно, вы думаете, что мошенники всегда будут хитрее вас и защититься от них сложно. Я тоже так думал, пока не усвоил одно простое правило: Если поступают подобные звонки, лучше ответить так: «Я перезвоню в банк и уточню информацию».

Слайд 6
Нажмите на «плей»

Тренер:
Дмитрий дал нам отличный совет. А в ваших рабочих тетрадях мы подготовили много полезной информации. Предлагаю подписать рабочую тетрадь и открыть ее на стр. 1

2. Разбор кейсов - 20 мин.
Цель: разбор реальных кейсов, выполнение задания в рабочих тетрадях для оценки начального уровня знаний

Для начала мы проверим, насколько сложно вас обмануть. В рабочей тетради на страницах 1-2 вы видите 8 кейсов. Это переписки в мессенджерах. Ваша задача – прочитать переписку и в конце каждого кейса ответить на вопрос: мошенники это или нет, закрасив кружок с ответом «ДА» или «НЕТ».

РТ, с.1-3

Слушатели самостоятельно выполняют задание 10 минут.
Далее тренер выводит переписки на экран и разбирает каждый кейс.

Итак, мы рассмотрели примеры сообщений, которые могут прийти от знакомых, коллег, бывшего начальника, из магазина и т.д. Кто может сказать, сколько среди них было сообщений от мошенников? Сколько кружков «ДА» вы закрасили?
Да, верно. Все эти сообщения от мошенников!
Теперь давайте разберём кейсы, чтобы лучше понять, как действуют мошенники и

как им противостоять. Вы можете делать записи на стр.3.	
Кейс 1. Переписка Ильи и его коллеги В этом кейсе телефон коллеги Ильи взломали мошенники. В такой ситуации нужно срочно связаться с коллегой: позвонить или отправить голосовое сообщение по рабочему телефону или в другом мессенджере. Не доверяйте переписке, в которой идет речь о деньгах, даже если вам пишет близкий человек. Используйте только свои банковские карты, если знаете их номера. Никогда не переводите деньги на чужие карты, не посоветовавшись со знакомыми.	Слайд 7 Слайд 8
Кейс 2. Переписка с бывшим начальником Вы могли давно уволиться, но кто-то продолжает писать вам, как будто вы всё ещё работаете. Для этого создаются фейковые аккаунты. Они могут содержать фото и личные данные вашего начальника, но номер телефона будет засекречен. Если вы сомневаетесь, позвоните начальнику по номеру телефона, который у вас мог остаться в записной книжке. Пишут с таких фейковых аккаунтов с целью запугать бывшего сотрудника и выманить у него деньги разными способами.	Слайд 9
Кейс 3. Сообщение от супруги (подруги) В данном случае мужчину насторожила сумма, которую попросила его жена. Он сразу понял, что это не она (она обычно просила больше). Чужая карта – снова маячок настороженности. Телефон жены был вскрыт!	Слайд 10
Кейс 4. Сообщение от незнакомого номера Сообщение о выигрыше в лотерею – типичное мошенничество, если вас просят что-то оплатить. Настоящие выигрыши перечисляются полностью за вычетом налога на доходы, который фирма платит за вас. Ничего не надо никому платить!	Слайд 11
Кейс 5. Сообщение от бывшего работодателя Снова сообщение от бывшего работодателя. А он ли это? Телефон засекречен? Смело блокируем!	Слайд 12
Кейс 6. Сообщение от нового знакомого в мессенджере Чтобы перевести деньги, достаточно знать номер телефона или номер карты получателя. Другую информацию сообщать опасно, так как ею могут воспользоваться мошенники. В данном случае запрашивается код CVV (3 цифры на обратной стороне). И да, к новым знакомым нужно относиться настороженно.	Слайд 13
Кейс 7. Сообщение от официального канала «Профессиональные Инвестиции» Если вы задумали инвестировать, то никаких переписок в мессенджерах быть не должно. Вы регистрируетесь на сайте известного брокера (например, Т-банк) и всю переписку ведете только в чате личного кабинета. Инвестирование может быть выгодным. Но больше 20-25% прибыли за год вам, скорее всего, не сможет предложить ни один брокер. Безумные проценты – это очень подозрительно и такое	Слайд 14

предложение может быть мошенничеством. Кейс 8. Сообщение в мессенджере от известного магазина Мошенники создают поддельные страницы известных брендов и общаются через мессенджеры. Не ведитесь на это! Заказывайте товары только через личный кабинет на официальном сайте. Иначе есть риск потерять деньги и не получить покупку.	Слайд 15
Кейс 9. Вовлечение в схему с дропами. Дроп или дроппер – человек, который выполняет задания дроповода. То, что ты получил задание, может быть понятно не сразу, ведь для этого у злоумышленников припасены различные схемы. Задания для дроппера: • перевести полученные деньги следующему участнику схемы; • снять полученные деньги в банкомате и передать их другому человеку; • выполнить услугу и получить за неё оплату «серыми» деньгами. Не оформляйте карты на своё имя с целью передачи другому лицу, не соглашайтесь снимать деньги с чужих карт с целью передачи незнакомым, даже если за это вам обещают вознаграждение.	Слайд 16
3. Виды финансового мошенничества - 25 мин. Цель: сформировать представление о видах финансового мошенничества и способов защиты от них.	
Сегодня мы обсудим основные виды финансового мошенничества. Их сложно запомнить, и каждый год появляются новые схемы. Наша задача – научиться распознавать угрозы для своих финансов и проверять поступающую информацию. Если что-то вызывает сомнения, лучше перепроверить. Не переводите деньги незнакомым людям, не сообщайте личные данные и не доверяйте кому попало.	
Давайте разберём несколько реальных примеров финансового мошенничества. А затем вы самостоятельно попробуете определить вид мошенничества в ещё нескольких кейсах. Помогать нам будут уже знакомые Ирина и Дмитрий.	Слайд 17
Откройте вашу РТ на странице 4. Вы видите схему «Виды финансового мошенничества». Сейчас мы подробнее разберем каждый блок, и ваша задача – обводить ручкой элементы, о которых мы будем говорить.	РТ, с.4
Существует мошенничество с банковскими картами, оно бывает офлайн и онлайн. Все виды мошенничества с банковскими картами связаны с тем, что вы сами сообщили свои данные для снятия денег или они были украдены кибермошенниками (мошенниками, причиняющими материальный или иной ущерб путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.). Были ли такие ситуации в вашей жизни? *(слушатели отвечают)*	
Виды офлайн мошенничества с банковскими картами:	

Скимминг – это когда на банкомат устанавливают специальное устройство (скиммер), которое считывает данные с вашей банковской карты (информацию с магнитной полосы и пин-код) и крадёт деньги с вашего счёта.	Слайд 18
Как вы думаете, как можно защититься от скимминга? *(слушатели отвечают)* Чтобы защититься от скимминга, соблюдайте следующие рекомендации: - Используйте банкоматы, расположенные в отделениях банков. - Обращайте внимание на подозрительные устройства на банкоматах. - Не вставляйте банковскую карту в подозрительные устройства. - Прикрывайте клавиатуру рукой при вводе пин-кода. - Регулярно проверяйте баланс банковской карты. - Немедленно сообщайте в банк, если подозреваете мошенничество. - Подключите услугу SMS-информирования о проведённых операциях по карте. Это позволит вам всегда быть в курсе действий с вашими средствами. - Используйте push-уведомления: они приходят мгновенно и позволяют контролировать ваши финансы в реальном времени.	Слайд 19
Ирина: Видов онлайн-мошенничества с банковскими картами много: Фишинг – кража личных данных и паролей карты через спамерскую рассылку. Вишинг – голосовой фишинг (звонки из банка и т.п.) с целью получить важную информацию. Смишинг – СМС от вроде бы надежного абонента с целью кражи ваших данных. Фарминг – перевод пользователей на фальшивый сайт с целью кражи информации.	Слайд 20 Нажмите на «плей»
Пролистать слайды с примерами Фишинга, вишинга, смишинга и фарминга.	Слайды 21-24
Давайте мы все эти способы будем называть одним словом: кибермошенничество.	
Как защитить себя от Кибермошенничества? *(ответы слушателей)* Есть общее правило покупок в интернете: покупать только на проверенных сайтах! Рекомендую установить антивирусные программы. Внимательно читайте адресную строку сайта. Не открывайте сомнительные письма. Никому не пересылайте свою личную информацию и данные банковских карт. Не экономьте при покупках на сомнительных сайтах, это может закончиться потерей денег.	Слайд 25
Друзья, ну как, успеваете? Все материалы останутся вам после занятия. Вы сможете еще раз их изучить. Еще я хочу рассказать вам о нигерийских письмах и других «письмах счастья» по поводу выигрышей в лотерею. Эх, если бы нам всем дядюшка из Америки оставлял миллион долларов в наследство. Как бы мы хорошо жили, не правда ли?	
Прочитайте письмо в вашей рабочей тетради на стр.5. *(Слушатели читают)* Какая информация в этом письме вас насторожила? В чем вы видите мошенничество в данном случае? *(слушатели отвечают)*	РТ, с.5 Слайд 26

В этом письме нужно обратить внимание на огромные суммы денег, на ломаный русский язык, на неправдоподобность ситуации в целом. Дальше последует просьба оплатить услуги адвоката еще ДО зачисления вам денег. Понятно, что никакого зачисления денег не будет. Запишите, пожалуйста, вывод в вашей рабочей тетради.	
Итак, с нами на связи снова Ирина. *Ирина:* Теперь поговорим о социальном манипулировании, или социальной инженерии. Это вид мошенничества для людей, которые всему верят и не проверяют информацию. Надеюсь, среди вас таких нет. Опытные мошенники эффективно манипулируют людьми, играя на их слабостях и особенностях. Они могут использовать разные технические средства только для того, чтобы установить контакт. А потом вы сами отдадите деньги, потому что мошенники «взломают» ваш мозг.	Слайд 27
Дмитрий: Мошенники часто притворяются сотрудниками полиции, Центробанка или ФСБ. Они могут запугивать или говорить, что вы делаете доброе дело, помогаете кому-то. Главное для них – получить ваши деньги.	Слайд 28
Тренер: Кроме того, мошенники могут выпрашивать деньги на лечение несуществующих или уже умерших больных детей, а также на помощь несуществующим животным. Доверчивых людей они обманывают, поскольку лишены совести и жалости.	
Давайте посмотрим ролик https://www.youtube.com/watch?v=quJoYsaVtiY Если вы хотите помочь нуждающимся, обратитесь в крупные проверенные фонды. Они отчитываются о каждом потраченном рубле жертвователей. Например, в МТС Банке сервис «Пожертвования» находится в разделе «Платежи».	Видео
Ирина: В социальных сетях тоже встречаются мошенники. Они могут не просто просить деньги, но и собирать информацию о вас. Например, если вы напишете, что едете с друзьями в Крым, сетевые воры могут решить, что ваша квартира какое-то время будет пустовать, и попытаются её обокрасть. Будьте осторожны и не делитесь лишней информацией. Если у вас несколько страниц в соцсетях, лучше разделить рабочую и личную информацию.	Слайд 29
Тренер: Еще хочу обратить внимание на махинации с вашим паспортом, который может попасть в руки мошенников. Какие манипуляции могут совершить мошенники с вашим паспортом? *(слушатели отвечают)* Верно, это и взятие кредита на ваше имя, и брак с незнакомым вам человеком, и махинации с недвижимостью. Я желаю вам, чтобы вы научились распознавать сомнительные сделки и никогда не подвергались атакам мошенников!	Слайд 30
Запишите в тетради главное из нашего разговора. Эти знания пригодятся вам в	

жизни. У вас 2 минуты. А теперь давайте закрепим полученные знания и поможем героям сделать правильный выбор. Нас ждёт практикум «Обмани меня, если сможешь».	РТ, с.5

4. Практикум «Обмани меня, если сможешь» - 25 мин.
Цель: сформировать насмотренность о видах финансового мошенничества и предложить способы защиты от них.

Сейчас я предлагаю каждому из вас взять по 1 карточке. *Слушатели берут по 1 карточке, выполняют задание (на подготовку дается 1 минута)* Задание: 1. Определить, мошенническая ситуация или нет. Подумать, какие последствия возможны. 2. Дать совет герою, что ему делать. *Обсудить каждую ситуацию. Начать с самого смелого слушателя. Тренер читает ситуацию и просит слушателя объяснить ее (ответить на вопросы).* **Ответы для тренера** Ответ на кейс 1: Не заподозрив подвоха, Анна перешла по ссылке и ввела свои учетные данные. Вскоре с ее банковского счета были списаны крупные суммы. К сожалению, мошенники могут посылать СМС и совершать звонки с телефонов, аналогичных реальным номерам банков. Ответ на кейс 2: Анна знала из урока по финансовой грамотности, что очень высокая доходность может означать ненадёжность компании. 30 % в месяц – это много. К тому же, при инвестировании доходность не гарантирована. Это могли быть мошенники. Анна не обратила внимания на сообщение. Ответ на кейс 3: Анна увидела выгодное предложение и сделала заказ. Когда посылка пришла, выяснилось, что товар некачественный и подделка. В таких случаях можно обратиться к закону о защите прав потребителей и вернуть товар в течение 7 дней после покупки онлайн. Если деньги не вернут, попробуйте запустить процедуру чарджбека (возвращение суммы, потраченной при оплате товара или услуги). Ответ на кейс 4: После того как Анна поверила и предоставила информацию, с её счёта были украдены средства. Не повторяйте ошибок Анны: никому не сообщайте данные	Слайд 31 Карточки к практ. заданию

своей банковской карты. Если у банка возникнут подозрения, он сразу заблокирует вашу карту.

Ответ на кейс 5:

Анна поняла, что стала жертвой мошенников. Она раньше никогда не инвестировала, но много читала об этом и знала, что общаться с брокером нужно только через личный кабинет. И что акции – это непростой инструмент, чтобы говорить об их высокой доходности. Доходность акций зависит от рынка.

Ответ на кейс 6:

Мошенники нашли кошелёк Анны и воспользовались личными данными из её паспорта, чтобы оформить кредиты на её имя. Теперь Анне приходится разбираться с последствиями этой ситуации. Кроме того, на банковской карте Анны не было лимита, и мошенники смогли потратить все 22 тысячи рублей, которые были на карте.

В подобных ситуациях рекомендуется:

- установить лимит на банковскую карту;
- не хранить большие суммы денег на карте, а переводить их на накопительный счёт или вклад;
- сразу блокировать карту при потере кошелька;
- не носить в кошельке копию паспорта;
- регулярно проверять свою кредитную историю на наличие непогашенных кредитов;
- заявить в полицию и банк при обнаружении кредита;
- в дальнейшем поставить самозапрет на взятие кредита без личного присутствия (эта возможность скоро появится благодаря новому закону).

Ответ на кейс 7

Позже выяснилось, что это был фальшивый фонд, созданный мошенниками.

Что нужно делать:

- проверять законность благотворительных организаций (сколько лет зарегистрированы, какие отзывы, есть ли отчёты о средствах);
- жертвовать напрямую в известные и проверенные фонды;
- не доверять эмоциональным историям без подтверждения.

Ответ на кейс 8

Сергей перевел деньги, но никакого выигрыша так и не получил.

Что нужно делать:

- Не верить сообщениям о выигрышах в лотереи, если вы не участвовали в ней.
- Не переводить деньги за обещанные призы.
- Проверять информацию о лотереях и организаторах.

Ответ на кейс 9

Вложив средства, Сергей потерял их, так как брокер оказался мошенником.

Что нужно делать:

- Проверять лицензии и репутацию брокерских компаний.
- Не доверять слишком высоким обещаниям доходов.
- Использовать только авторизованные и проверенные брокерские платформы.

Ответ на кейс 10

Оплатив покупку, Сергей не получил обещанную криптовалюту. Обращение в полицию также не привело к успеху. Криптовалюта – это деньги, за оборот которых государство не отвечает.

Что нужно делать:

- Использовать только официальные и проверенные криптовалютные биржи.
- Не доверять неизвестным онлайн-магазинам криптовалюты.
- Проверять отзывы и рейтинги перед совершением покупки.

Ответ на кейс 11

Сергей так и не получил кредит, потому что кредитор оказался мошенником. У него не было лицензии на операции с деньгами, и он просто собирал с людей деньги за свои услуги. Кредит нужно брать только в проверенных организациях, тщательно изучая договор и условия кредитования.

Ответ на кейс 12

Сергей перезвонил Дмитрию и выяснил, что тот потерял телефон. А девушки у него пока нет. Поэтому деньги не нужны. Сергей проявил бдительность и поступил правильно.

5. Просмотр видео - 7 мин

Цель: сформировать насмотренность о видах финансового мошенничества и предложить способы защиты от них.

В завершение нашего занятия я предлагаю посмотреть видео «Письмо счастья». *Обсудить со слушателями действия героев.*
https://www.youtube.com/watch?v=ILvYbw96-5k

Видео

Если времени не остается – можно попросить слушателей посмотреть видео дома (в РТ на стр. 5 есть ссылка на видео)

6. Завершение занятия - 3 мин

Цель: закрепить изученный материал, сделать выводы. Получить домашнее задание.

Вот и подошло к концу наше занятие. Я уверена, что вы сегодня узнали много нового и полезного.

Я благодарю вас за активное участие и надеюсь, что мы увидимся на следующем занятии. Дома я попрошу вас следовать советам на каждый день, которые помогут вам сохранить ваши денежные средства (РТ с. 6-9)

А теперь давайте похлопаем себе за активное участие! Ещё раз! Вы молодцы!